IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 058556-0109

Applicant:	Yasumasa UYAMA
Title:	PROTECTED COMMUNICATION SYSTEM
Application No.:	10/021,052
Filing Date:	12/19/2001
Examiner:	Poltorak, Piotr
Art Unit:	2134

PERFECTION OF CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country was requested in a claim for convention priority that was filed on March 15, 2002, where the right of priority provided in 35 U.S.C. §119 was claimed.

Further to that claim of priority, in order to perfect that claim, filed herewith is a verified translation of the original foreign application:

- Japan Patent Application No. 2000-388921 filed December 21, 2000.

Respectfully submitted,

October 13, 2006
Date

Phillip J. Articola
Registration No. 38,819

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5300
Facsimile: (202) 672-5399

CERTIFICATION

I, Shin-ichi Iizuka, of 29-9, Higashi 3-chome, Kunitachi-shi, Tokyo 186-0002, Japan, hereby certify that I am the translator of the accompanying certified official copy of the documents in respect of an application for patent filed in Japan and of the official certificate attached thereto, and certify that the following is a true and correct translation to the best of my knowledge and belief.

Shin-ichi Iizuka

Dated this 3rd day of October, 2006

【Document】 Patent Application

【Reference No.】 YU2000-01

【Address】 To Commissioner, Patent Office

【Int.Patent Class】 H04K 1/00

【Inventor】

【Address】 Room 504, 30-15, Kurihama 8-chome,
Yokosuka-shi, Kanagawa,
239-0831 Japan

【Name】 Yasumasa Uyama

【Applicant for Patent】

【Identification No.】 300085864

【Name】 Yasumasa Uyama

【Indication of Official Fee】

【Book No. of Amount of Money】 123963

【Amount of Money of Payment】 21,000 yen

【List of Attached Document(s)】

【Document】	Specification	1
【Document】	Drawings	1
【Document】	Abstract	1

【Necessary or unnecessary of Proof】 Necessary

[Document] SPECIFICATION

[Title of the Invention]

ORDERED PAIR SYSTEM ENCIPHERED COMMUNICATION

[Scope of Claim]

[Claim 1] A method of protected communication utilizing cipher by an information equipment capable of using memory device and operation device, wherein:

a communication using cipher is automatically performed according to an enciphering method (Csr) and a deciphering method (Psr) determined uniquely corresponding to an ordered pair (S, R) of sender (S) and receiver (R): and

the enciphering method corresponding to the ordered pair (S, R) is designated freely by the receiver (R).

[Claim 2] A communication software realizing the method of protected communication according to Claim 1, having a list of identification symbol (e-mail address or telephone number) with a designation column for enciphering and a designation column for deciphering, wherein:

an enciphering is automatically performed upon transmission according to a method designated by the receiver of information: and

a deciphering is automatically performed upon reception according to the deciphering method corresponding to the sender.

[Claim 3] A form of cipher software enabled to be divided into an enciphering part and a deciphering part, wherein:

the freedom of redistribution of the enciphering part is approved: and

the freedom of redistribution of the deciphering part is disapproved.

[Claim 4] A method of distributing information at a fee utilizing Claims 1, 2, and 3, wherein information is distributed by enciphering, at least having a strength higher than what is requested by clients.

[Detailed Description of the Invention]

[0001]

[Technical Field]

The present invention relates to a method of enforcing protected communication over the network.

[0002]

[Prior Art]

A method of enciphering information to be transmitted may be given as a technology for ensuring safety of communicating information, however, it requires cumbersome procedure. Also, readily utilizing new and powerful enciphering system adapting to the development of the deciphering technology of cipher is currently at a difficult situation.

[0003]

[Tasks to be Achieved by the Invention]

The situation does not allow simple and automatic performance of safe and reliable communication of information, and a large number of people are holding anxiety toward the network society and are hesitant toward active participation. A network society must be a place where everyone may securely and readily participate.

[0004]

[The object of the invention]

The object of the present invention is to revise the method of protected communication in order to allow everyone to utilize the encipher technology with ease, and also enabling easy renewal to a new cipher method considering the development of deciphering technology.

[0005]

[Means to Achieve the Task]

An enciphering method and a deciphering method is uniquely determined corresponding to an ordered pair of the sender and receiver, and function of a communication software is expanded to perform the ciphered communication according to this method. The enciphering and deciphering are performed automatically by

utilizing an address book having a designation column for cipher method.

A method enabling easy renewal to a new cipher system adapting to the development of deciphering technology is to be realized. The receiver of the information freely selects the cipher method. The structure of the cipher method is divided into two parts, enciphering part and deciphering part, and the freedom of redistributing the enciphering part is approved. However, the redistribution of the deciphering part is enabled to be prohibited. By so doing, producing and merchandising of cipher software on commercial bases are financially guaranteed, and the cipher software of high quality will be supplied steadily.

This method may be utilized for communication using telephones, but a memory device and an operation device needs to be added to the current telephone machines. Further, the standard needs to be unified on some items.

Thereupon, matters regarding electronic mail (referred simply as e-mail hereinafter) over the internet, which can be realized immediately using current hardware will be focused in the description hereinafter.

[0006]

[A Law of Nature Utilized in this Invention]

There is only two ways of arranging 2 objects X and Y in order, (X, Y) and (Y, X), and no other way is available. The present invention is realized utilizing this law of nature.

[0007]

[Embodiment]

[0008]

[The Uniqueness of Address and the Ordered Pair]

In the internet society, identification codes that specify individuals such as e-mail address and IP address exist. By specifying the sender and receiver of an information, the ordered pair can be determined using the two e-mail addresses (sender, receiver).

A structure is created in order to determine the enciphering program corresponding to the ordered pair. When (X, Y) represents communication from Mr. X to Mr. Y, the receiver Mr. Y freely determines the enciphering method to be used. Further, information from Mr. X to Mr. Y is enciphered automatically using a pre-set method determined by Mr. Y.

An enciphering method relied upon by Mr. Y does not necessarily be the technology Mr. X can rely on. Therefore when Mr. X receives information from Mr. Y, an ordered pair (Y, X) determines the enciphering method, in other words, a pre-set enciphering method determined by Mr. X regarding Mr. Y, is used for enciphering upon transmission. This will be possible considering the following aspects.

[0009]

[Expanding the Address Book]

Currently, a software used in communicating over the internet has an address book storing names, e-mail addresses, organizations, telephone numbers, and the like. This address book is expanded with addition of 4 items, enciphering key, enciphering software, deciphering key, and deciphering software.

For example, changes are made as described in the following.

Mr. Akiyama's address book

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCax	Cax	KPxa	Pxa
Mr. Ito	Ito@asn	KCai	Cai	KPia	Pia
Mr. Saito	Saito@uu	KCas	Cas	KPsa	Psa
Mr. Baba	Baba@yy	KCab	Cab	KPba	Pba

[0010]

[The Function of the Software at the Time of Communication]

Suppose Mr. X transmits information to Mr. Y. At this time, the ordered pair (X, Y) is determined and an enciphering method corresponding to this ordered pair can be uniquely determined. Based on this fact, the software must function as described hereinafter.

[0011]

[The Function at the Time of Transmission]

Once the transmitting information is given, the destination address of the e-mail is searched, and the columns for enciphering key and enciphering software are looked up. If those information are designated, then the designated enciphering software is read out by using the enciphering key and the transmission content as an index, and the transmission content is enciphered.

The enciphered information is transmitted as an attachment file of a blank e-mail, listing only the address of the destination and the address of the sender.

Obviously, for people not listed in the address book, or people listed in the address book but have no designation of the enciphering items, the e-mail will be sent as it is without enciphering. Refer to figure 1 for function at the time of transmission.

[0012]

[The Function at the Time of Reception]

At the time of receipt, the e-mail address of the sender is looked up in the address book. If a deciphering key and a deciphering software are given under the column of the sender, the deciphering program is read out by using the deciphering key and the attachment file as an index, and performs deciphering. Then the information free of enciphering is displayed.

Obviously, regarding e-mails from people not listed in the address book, or those listed in the address book but has no designation in the deciphering items, the e-mail is opened regularly. A software or a hardware having such function is to be produced.

Refer to figure 2 for function at the time of receipt.

[0013]

[The Types and Characteristics of the Encipher that can be Used]

There are 2 major types of enciphering, a secret key system and an open key system, and both types can be used. There are approximately 100 types of enciphering software that receives high review from the society and are acknowledged as effective by the experts.

An enciphering key and an enciphering software realized as one common body creates a practical problem. The size of enciphering key is approximately 1K bytes, but unified key and software will be approximately 1M to 10 M bytes. In order to store data of this size for 10,000 people, 100G bytes will be required, and it will be difficult for a hard disk having approximately 10G bytes. If a common enciphering software may be used, then even when there are enciphering keys for 10,000 people, the size would only be approximately 10M bytes.

In theory, the enciphering key and enciphering software need not be separated, but for the reason that it is more suited for the current hardware situation, a method separating the enciphering key and the enciphering software will be described hereinafter.

Preferably, a commercial enciphering software having the following structure is produced.

(1) Having an enciphering key creation function, and the freedom of distributing the key is approved.

(2) A freedom of redistributing the enciphering software is approved.

(3) Having a deciphering key creation function.

(4) The redistribution of the deciphering software can be prohibited.

Provided that the above described conditions (1) to (4) are fulfilled, then both secret key system and open key system may be used. It is not difficult to produce enciphering software having such structure.

If the redistribution of the deciphering software can be prohibited, then each of

the enciphering software users will be required to purchase a software, and this allows production and merchandising of the software on commercial bases and enables the development of high quality enciphering software.

The enciphering software may be self-produced. However, producing a safe enciphering software requires considerable amount of time and effort. Since numerous variations of enciphering software already exist, and Japan leads the world in some aspects, a realistic choice would be to select one that receives high review from the society.

[0014]

[A Case Using the Secret Key Cipher System]

When using the secret key system, the secret key and the enciphering software would need to be distributed beforehand. As an example, a case using Caesar enciphering system is described from hereinafter.

Mr. Akiyama has decided to use Caesar enciphering system, and the information from Mr. Ito is to be enciphered using the enciphering key (-1), and the information from Mr. Saito is to be enciphered using the enciphering key (2).

Mr. Akiyama's address book

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCax	Cax	25	P
Mr. Ito	Ito@asn	KCai	Cai	1	P
Mr. Saito	Saito@uu	KCas	Cas	-2	P
Mr. Baba	Baba@yy	KCab	Cab	22	P

Mr. Akiyama sends the enciphering key and the enciphering software (C) to Mr. Ito and Mr. Saito. Mr. Ito and Mr. Saito register the enciphering key and the software to

the enciphering column of their own address book. The address book of Mr. Ito and Mr. Saito is shown in the following.

Mr. Ito's address book

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCix	Cix	KPxi	Pxi
Mr. Akiyama	Akiyama@ss	(-1)	C	KPai	Pai
Mr. Saito	Saito@uu	KCis	Cis	KPsi	Psi
Mr. Baba	Baba@yy	KCib	Cib	KPbi	Pbi

Mr. Saito's address book

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCsx	Csx	KPxs	Pxs
Mr. Ito	Ito@asn	KCsi	Csi	KPis	Pis
Mr. Akiyama	Akiyama@ss	2	C	KPas	Pas
Mr. Baba	Baba@yy	KCsb	Csb	KPbs	Pbs

The communication from Mr. Ito to Mr. Akiyama (IBM) is enciphered by key (-1) and becomes (HAL). The cryptogram (HAL) from Mr. Ito is deciphered back to (IBM) with the key of Mr. Akiyama corresponding to the communication from Mr. Ito.

The communication from Mr. Saito to Mr. Akiyama (IBM) is enciphered by key (2) and becomes (KDO). The cryptogram (KDO) from Mr. Saito is deciphered back to (IBM) by the key (-2).

In other words, the alphabets are progressed in the alphabetical order by the value of the enciphering key, and it is brought back by the number shown by the value of the deciphering key.

[0015]

[A Case Using the Open Key Cipher System]

When using the open key system, the open keys need to be sent to all the intended people from whom the receipt of enciphered information is desired. Also, the same enciphering software should be distributed. Of course, there are numerous embodiment variations amongst the open key system, and therefore, it is possible to utilize different open key system enciphering software for each intended person.

As an example, a case using a discrete logarithm is described hereinafter. Prime numbers p, q are selected, and is set as n=pq. Then, K=1cm (p-1, q-1) is set and number d is selected so that gcd (d, K)=1. Following, ed=1 (mod K) is set and an integer e is calculated so that 0<e<K. Mr. Akiyama discloses e and n, and sends the enciphering software (C). d is kept secret and is registered to the address book along with n.

Mr. Akiyama's address book.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCax	Cax	d, n	PS
Mr. Ito	Ito@asn	KCai	Cai	d, n	PS
Mr. Saito	Saito@uu	KCas	Cas	d, n	PS
Mr. Baba	Baba@yy	KCab	Cab	d, n	PS

Suppose Mr. Akiyama sends the enciphering key and the enciphering software to Mr. Ito and Mr. Saito. The address books of Mr. Ito and Mr. Saito are shown in the following.

Mr. Ito's address book.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software

X Company	xcp@kabu	KCix	Cix	KPxi	Pxi
Mr. Akiyama	Akiyama@ss	e, n	C	KPai	Pai
Mr. Saito	Saito@uu	KCis	Cis	KPsi	Psi
Mr. Baba	Baba@yy	KCib	Cib	KPbi	Pbi

Mr. Saito's address book

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCsx	Csx	KPxs	Pxs
Mr. Ito	Ito@asn	KCsi	Csi	KPis	Pis
Mr. Akiyama	Akiyama@ss	e, n	C	KPas	Pas
Mr. Baba	Baba@yy	KCsb	Csb	KPbs	Pbs

Suppose a numeral x is to be transmitted, the enciphering software C of Mr. Ito and Mr. Saito, calculates $x^e \equiv c \pmod n$ using e and n, and c is transmitted to Mr. Akiyama. The receiver, Mr. Akiyama obtain x from $c^d \equiv x \pmod n$. In other words, x is obtained by using the law of n and by calculating c to the power of d.

[0016]

[Distribution Method of Enciphering Key and Enciphering Software]

It is required to have the sender of information to own the enciphering key and the enciphering software beforehand. There are various ways of delivering, such as, giving the information saved on the floppy disk in person, mailing such disk, and transmitting over the network by enciphering the secret key with the open key system.

[0017]

[Registration of Enciphering Key and Enciphering Software]

The receiver of the enciphering key and the enciphering software register them in the address book. For example, suppose that Mr. Akiyama has decided to use enciphering for communication with Mr. Ito. The enciphering method is determined

corresponding to the ordered pair (Mr. Ito, Mr. Akiyama). The enciphering method when Mr. Akiyama receives the communication from Mr. Ito is set to be C (i, a). Mr. Akiyama meets with Mr. Ito, and delivers the enciphering software (Cia) and the enciphering key (KCia) in person. Mr. Ito registers the enciphering software and the enciphering key in the address book under Mr. Akiyama, and saves the enciphering key and the enciphering software in the hard disk.

Mr. Ito's address book will be as follows.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu				
Mr. Akiyama	Akiyama@ss	KCia	Cia		
Mr. Saito	Saito@uu				
Mr. Baba	Baba@yy				

[0018]

[Registration of Deciphering Software]

Mr. Akiyama has determined the enciphering method for receiving communication from Mr. Ito, and by this, the deciphering key (KPia) and deciphering software (Pia) is determined. The determined deciphering information is registered in Mr. Akiyama's address book under Mr. Ito's deciphering key and deciphering software columns.

Mr. Akiyama's address book will be as follows.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu				

Mr. Ito	Ito@asn			KPia	Pia
Mr. Saito	Saito@uu				
Mr. Baba	Baba@yy				

By this address book, Mr. Akiyama can receive communication from Mr. Ito in an enciphered form using (Cia). Also, the received information is automatically deciphered by (Pia).

Also, Mr. Akiyama may use the same enciphering method and same enciphering key for communication with other individuals apart from Mr. Ito. Further, the communication among other individuals may be performed using the same enciphering software, and different enciphering keys.

Also, a completely different method may be used to perform enciphered communication. This is because the ordered pair of the sender and the receiver determines the enciphering method and the embodiment mode. Similarly, it is clear that Mr. Ito may select a different enciphering method for receiving information from Mr. Akiyama.

[0019]

[The Significance of Prohibiting the Redistribution of the Deciphering Software]

By setting the enciphering software not to function as a deciphering software simultaneously, the users purchasing the enciphering software and utilizing this method each needs deciphering software, and are each required to purchase an enciphering software individually. This is due to prohibition of deciphering software redistribution. This guarantees the commercial development of the enciphering software, and thus becomes the economical base for safer communication. The development of enciphering software requires a long-term research, and a high quality enciphering software cannot be developed without economical guarantee.

[0020]

[The Uniqueness in the Names of Enciphering Software]

Different enciphering software given the same name will create problem upon storing into the hard disk. Therefore, a unique identification symbol (such as the e-mail address and the like) of the enciphering software developer should be used as the name for the enciphering software in order to avoid conflict of names.

[0021]

[Industrial Utility]

Suppose a security company (X company) provides information for the clients at a fee. Also suppose that a client has an interest in the automobile companies. For that client, information would be considered valuable even to purchase at a high price if an automobile company's development information for a new car were delivered solely for that individual.

However in reality, the delivery of this information that the client would like only himself/herself to know may be in danger of theft or falsification, and leaves an anxiety. Therefore, suppose the X Company has employed this system.

The list of addresses of the client for X Company is as follows.

Name	The client's address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
Mr. Akiyama	Akiyama@ss	KCxa	Cxa	KPax	Pax
Mr. Ito	Ito@asn	KCxi	Cxi	KPix	Pix
Mr. Endo	Endo@kk	KCxe	Cxe	KPex	Pex
Mr. Yamada	Yamada@yama	KCxy	Cxy	KPyx	Pyx

X Company delivers information of economical field of interest to the clients at a fee. As a general rule, the client determines the enciphering method, but it is also necessary for the X Company to introduce approximately 10 variations of enciphering software receiving high social review. In turn, the X Company determines the enciphering method for receiving orders and the like from the clients. The methods may

be changed according to the purchasing power of the clients.

If possible, producing as many deciphering keys as the number of clients would be convenient. However, a deciphering software that enables the use of different deciphering keys for the client but allowing the use of one common deciphering software would be preferred. Here also, the merit of enabling the separation of the deciphering key and the deciphering software can be seen.

A valuable economical information would be preferable to be sent solely for oneself, and would like to prevent this information from being tapped or receive falsification over the network. This method allows the protection of information solely for oneself at the clients' responsibility. This can add further additional value added to the information. This is an essential method of delivering information of economically high in value.

[0022]

[The Use by an Individual]

Following shows the address book of an individual utilizing this method. When used by an individual, the economical burden needs to be considered.

For the open key enciphering, only one type of deciphering key and deciphering software is required, since the same enciphering key can be distributed. Also a different open key system can be employed for business communication and for communication amongst friends.

For the secret key system, a different secret key is produced for each intended person, and the corresponding deciphering key is saved in the address book under the deciphering column. The resources such as the hard disk can be saved since the same enciphering software and the same deciphering software may be used for different keys. Of course, the enciphering method may be changed depending on the communication partner.

An enciphering software will be relatively large in size if it is combined with the enciphering key as one body, then enough amount for number of people in the

address book is required to be prepared in the hard disk. As the number of people increases, the memory becomes insufficient for the hard disk having approximately 20G bytes. Therefore, the enciphering keys, small in size, may be prepared as many as the number of people listed in the address book, but the enciphering software, large in size, is preferred to be used commonly.

There are approximately 100 enciphering software currently accepted as being effective. Only 100 types need to be placed in the hard disk, if the enciphering software can be utilized commonly. Also, it is possible to distribute the enciphering software alone, as a supplement to a magazine and the like. Therefore, obtaining the software in such a manner and exchange only the enciphering keys may be considered as a realistic method.

Mr. Akiyama's address book.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCax	Cax	KPxa	Pxa
Mr. Ito	Ito@asn	KCai	Cai	KPia	Pia
Mr. Saito	Saito@uu	KCas	Cas	KPsa	Psa
Mr. Baba	Baba@yy	KCab	Cab	KPba	Pba

Mr. Ito's address book.

Name	Address	Enciphering key	Enciphering software	Deciphering key	Deciphering software
X Company	xcp@kabu	KCix	Cix	KPxi	Pxi
Mr. Akiyama	Akiyama@ss	KCia	Cia	KPai	Pai
Mr. Saito	Saito@uu	KCis	Cis	KPsi	Psi
Mr. Baba	Baba@yy	KCib	Cib	KPbi	Pbi

The function of the communication software of this system is described

hereinafter. Upon transmitting an e-mail, the destination address and the address of the sender are determined first, and then, the ordered pair of sender and receiver is determined. The information will be enciphered automatically using an enciphering method corresponding to this ordered pair.

On the receiver's side, an ordered pair given by the address of the sender and the own address, which is the destination address, determines a deciphering method and the transmitted enciphered information is automatically deciphered.

For example, Mr. Akiyama determines the enciphering method to be used for receiving information from Mr. Ito. Mr. Akiyama prepares the enciphering key (KCia), enciphering software (Cia), deciphering key (KPia), and deciphering software (Pai) to be used in communication with Mr. Ito, and among them, information regarding the enciphering key (KCia) and enciphering software (Cia) is sent to Mr. Ito beforehand. Mr. Ito registers the enciphering key and the enciphering software in his address book under Mr. Akiyama's column.

An e-mail from Mr. Ito to Mr. Akiyama will be enciphered by enciphering method (Cia) and enciphering key (KCia), determined by Mr. Akiyama. The communication software of Mr. Akiyama receiving this e-mail, can make the distinction between the sender's address and the own address, and automatically selects the deciphering key (KPia) and the deciphering method (Pia), and deciphering is performed using this method.

On the other hand, Mr. Ito determines the enciphering method for receiving information from Mr. Akiyama. Of course, Mr. Ito may determine this method freely. Mr. Ito prepares the enciphering key (KCai), enciphering software (Cai), deciphering key (KPai), and deciphering software (Pai) to be used in communication with Mr. Akiyama, and among them, information regarding the enciphering key (KCai) and enciphering software (Cai) is sent to Mr. Akiyama beforehand.

An e-mail from Mr. Akiyama to Mr. Ito will be enciphered by enciphering method (Cai) and enciphering key (KCai), determined by Mr. Ito. Mr. Ito, receiving this

e-mail, uses deciphering key (KPai) and deciphering software (Pai) for Mr. Akiyama and deciphers the information.

[0023]

[Renewal of Enciphering Method]

The enciphering technology is improving at an amazing speed, and simultaneously, the deciphering technology is improving. One enciphering method is considered to be safe for 5 years at most. Therefore, enabling the receiver of information to freely renew the enciphering technology used would be needed.

According to this system, the receiver of information may freely perform renewal. Thus, the cipher technology of highest quality available at that time can be selected as long as the financial situation of the user allows.

An individual deciding to use a new enciphering method purchases new enciphering software, distributes the enciphering part to people listed in the address book, and request registration renewal. Also, renew the registration content of the deciphering part of the own address book.

Of course, there are people only needing simple enciphering, and also people not needing enciphering, but the fact that a person determines by his/her will, the enciphering method suited for the value of the information handled, just like a person choosing a key to his/her own room, is important.

[0024]

[Expanding the functions]

It is possible to utilize a plurality of columns for enciphering and deciphering, and perform multiple enciphering. Especially for providing information at a fee, apart from enciphering method determined by the client, an enciphering method considered to have the minimal strength by the company, should also be employed, and at least encipher the information twice.

[0025]

[A Case of a Telephone]

When using this method on telephone, several communication standards need to be determined. First, standardizing the sampling rate at the time of digitalization of voice. Secondly, the digitalized voice is enciphered per certain amount and the standardization regarding the amount.

Provided that these 2 points are determined, then, by utilizing caller identification feature, the enciphering determined by the ordered pair of the telephone numbers of the transmitter and the receiver enables the protected communication in case of the telephones as well.

In case of a home telephone, interlocking a memory device and an operation device is simple, and there is no power problem, therefore the only problem that needs to be solved is the processing speed of enciphering and deciphering.

In case of a mobile telephone, a memory stick and the like can solve a problem regarding the memory device. And simplifying the enciphering method can solve the large size of operation device.

For example, suppose that the data is enciphered per every 1,024 bit. The enciphering key and the deciphering key are set as a sentence as long as the length of this bit value, and both the transmitter and the receiver uses the same sentence. Suppose that the enciphering method and the deciphering method is XOR. Both enciphering and deciphering can be realized as the XOR per 1,024 bits of the key sentence and the digital data. The sentence can be written in the memory device. The use of a full-scale operation device is not needed, for a simple circuit can realize XOR alone. Each person can choose a sentence of their preference and have the other person register that sentence.

As the third and remaining problem, the production of a telephone machine interlocked with memory device and operation device can be given. This will arise a new demand. Producing and merchandising such computer-like telephone machine may contribute to the economical recovery of Japan. The development of a full-scale operation device small enough to be used in a mobile phones will take some time.

[0026]

[The Effect of the Invention]

This method of protected communication realizes individualized form of protected communication for each of the ordered pair of sender and receiver. The enciphering method is determined by the receiver himself/herself. Therefore the users can protect the receiving information at their own responsibility. Further, a method considered to be the most reliable enciphering method by the user can be selected, and therefore the users can participate in the network society free from anxiety.

Since the information can be delivered safely, transmission and reception of information high in economical value may be performed without anxiety. This method will function efficiently as a base for distributing information at a fee.

The users are solely responsible for determining the enciphering method, so the network participation will assume self-responsibility, and thus create independent and positive attitude towards participating in the network society. Therefore, subjective and positive international exchange is enabled.

The scale of commercial development or merchandising of enciphering software will increase. The theory of cipher or production aspect of software will require mathematical theory, and everyone can confirm the usefulness of mathematics. The mathematical ability of the Japanese will be utilized in improving safety, and thus contribute to the world.

Also, if this method were to be employed in telephones, telephone machine itself needs to be produced anew, and therefore creates new demand. If this new telephone machine were to be placed in all homes, it will be the same as all homes in Japan being connected by computers, and new service potential will be infinitely broadened.

[Brief Description of the Drawing]

[Figure 1] A figure showing the function of the present communication software at the

time of transmission.

[Figure 2] A figure showing the function of the present communication software at the time of reception.

[Explanation of Terms]

1. Enciphering part

There are various types of software that creates cryptogram from plain text such as, comprising of enciphering key and enciphering software, does not utilize enciphering key, interlocking enciphering key into enciphering software as one body, and the like. The enciphering part refers to a part that has function of enciphering a plain text into cryptogram.

2. Deciphering part

There are various types of software that converts cryptogram into plain text such as, comprising of deciphering key and deciphering software, does not utilize deciphering key, interlocking deciphering key into deciphering software as one body, and the like. The deciphering part refers to a part that has function of deciphering a cryptogram into plain text.

3. Cipher software

A term representing enciphering software, enciphering key, deciphering software, and deciphering key used in enciphered communication as a whole.

4. Caesar cipher

A cipher that is said to be utilized by Caesar in the Roman era, and is characterized by remainder calculation having 26 as the law.

5. Discrete logarithm

When a relationship of $\alpha \text{^} e \equiv a \pmod{p}$ exists upon Zp, then e is called a discrete logarithm of a.

6. XOR

XOR represents exclusive or. The calculation will be: 1XOR1=0, 1XOR0=1,

and 0XOR0=0.

7. Deciphering

A process of restoring the original plain text from a cryptogram.

[Document] ABSTRACT OF THE DISCLOSURE

[Abstract of the Disclosure]

[Object] To strengthen the degree of safety in communication.

[Means of Solving]

(1) A protected communication by enciphering method uniquely determined corresponding to an ordered pair (S, R) of sender and receiver.

(2) A communication software having an address book with an enciphering designation column and a deciphering designation column, wherein enciphering and deciphering is performed automatically according to the content of the designation column.

(3) A cipher software capable of dividing into enciphering part and deciphering part, wherein the enciphering part is authorized of freedom of redistribution.

[Effects] A protected communication realized utilizing the methods 1, 2, and 3, allows renewal to a highly reliable cipher method using new theory adapting to the development of deciphering technology, and information needing to be kept a secret can be provided over the network without fear of tapping or receiving falsification. Information provided at a fee with added value of safety to information can be provided. By authorizing redistribution of only the enciphering part, the enciphering program may be developed commercially. Employing this method on telephones will dig up demand for the new telephone machine. Above all, each individual will subjectively participate in the network society.

Fig. 1

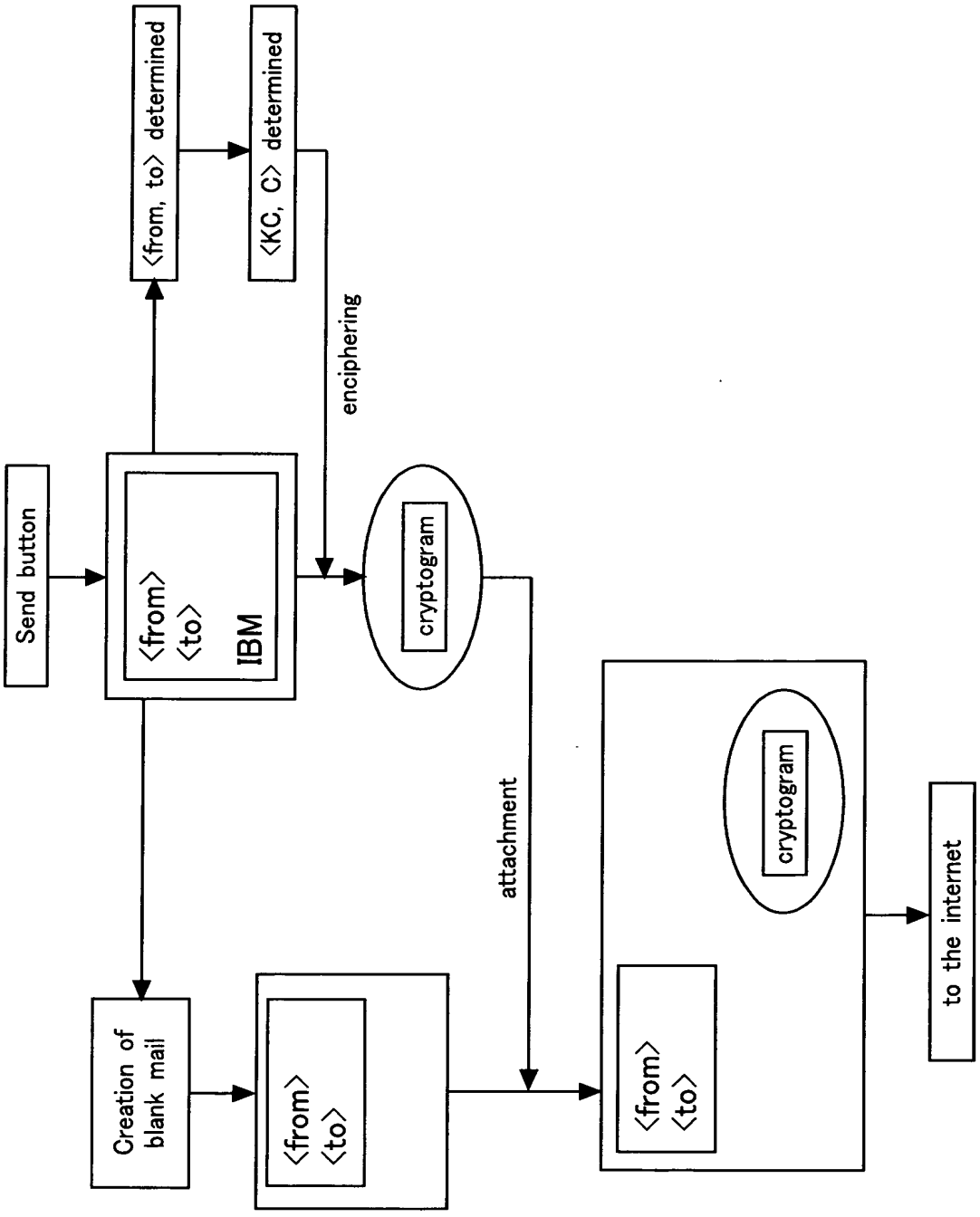
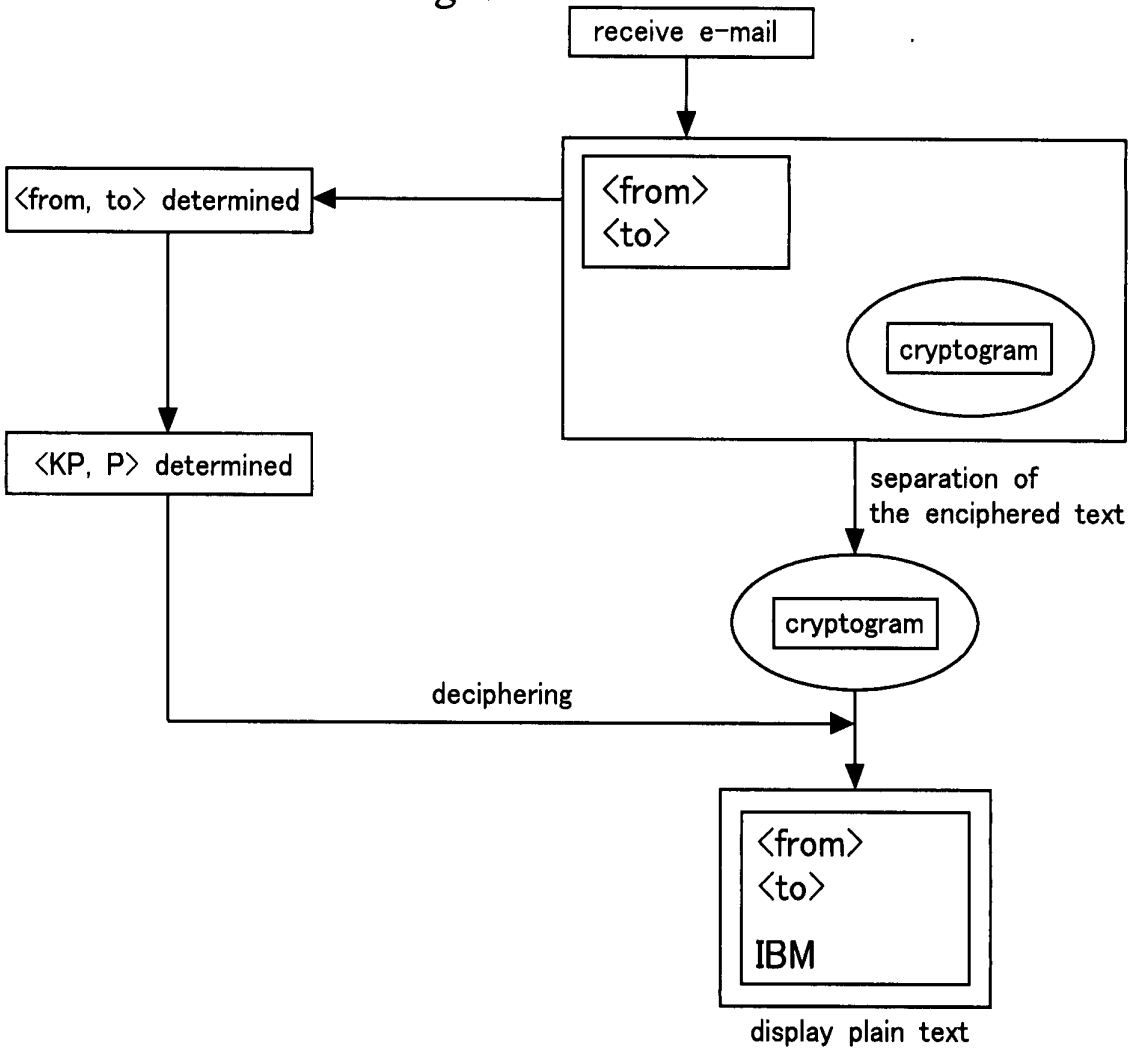


Fig.2


receive e-mail
<from>
<to>
cryptogram
<from, to> determined
<KP, P> determined
separation of
the enciphered text
cryptogram
deciphering
<from>
<to>
IBM
display plain text